Secondary Constructions of Bent Functions and Highly Nonlinear Resilient Functions

Fengrong Zhang * Claude Carlet † Yupu Hu ‡ Wenzheng Zhang §

November 20, 2012

Abstract

In this paper, we first present a new secondary construction of bent functions (building new bent functions from two already defined ones). Furthermore, we apply the construction using as initial functions some specific bent functions and then provide several concrete constructions of bent functions. The second part of the paper is devoted to the constructions of resilient functions. We give a generalization of the indirect sum construction for constructing resilient functions with high nonlinearity. In addition, we modify the generalized construction to ensure a high nonlinearity of the constructed function.

Keywords : Boolean function, bent function, resilient function, high nonlinearity.

1 Introduction

Bent functions were introduced by Rothaus in 1976 as an interesting combinatorial object with the important property of having optimal nonlinearity [36]. Since bent functions have many applications in sequence design, cryptography and algebraic coding [26, 33], they have been extensively studied

*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, P.R. China (e-mail: zhfl203@cumt.edu.cn)

†Department of Mathematics, LAGA, UMR 7539, CNRS, Universities of Paris 8 and Paris 13, 93526 Saint-Denis cedex 02, France (claude.carlet@inria.fr)

‡State Key Laboratory of Integrated Services Networks, Xidian University, Taibai Road 2, Xi'an 710071, P.R. China (e-mail: yphu@mail.xidian.edu.cn)

§Science and Technology on Communication Security Laboratory, the 30th Research Institute of China Electronics Technology Group Corporation, Chengdu 610041, P.R. China (e-mail: zwz85169038@sina.com)

during the thirty last years [3, 4, 13, 18, 20, 23, 31, 41]. In terms of sequence design, several binary bent sequences were constructed by using the bent functions [32, 33]. Binary bent sequences can be good candidates for many commutation systems such as code-division multiple-access systems, radar systems, and synchronization systems in that they have optimal correlation and balance property [25, 32, 33]. In addition, bent functions can also be used to construct highly nonlinear balanced functions [19].

With regard to constructions of bent functions, there are two kinds of constructions: primary constructions (designing functions without using known ones) and secondary constructions. The primary constructions mainly include the Maiorana-McFarland (M-M) class [18], the partial spreads (PS) class [18] and Dobbertin gave a construction of a class of bent functions which leads to some elements of M-M class and of PS class as extremal cases [19]. The secondary constructions mainly include direct sum construction [18], Rothaus' construction [36], indirect sum construction [9]. Moreover, there are some constructions of bent functions proposed in [3, 5, 8, 16, 24]. However, although many concrete constructions of bent functions have been discovered, the general structure of bent functions is still unclear. In particular a complete classification of bent functions seems hopeless today.

Resilient functions have important applications in the nonlinear combiner model of stream cipher [1, 39, 42]. Over the last decades, much attention was paid to the construction of highly nonlinear Boolean functions in the cryptographic literature [7, 22, 34, 37, 43, 46, 44, 45]. In terms of constructions of resilient functions, there are also two kinds of constructions which are primary constructions and secondary constructions. The primary constructions mainly include Maiorana-McFarland's construction [1], generalizations of Maiorana-McFarland's construction [7, 10], Dobbertin's construction [19, 38] and other constructions [21, 46]. In addition, the simple secondary constructions mainly include direct sum of functions [39], Siegenthaler's construction [39], Tarannikov's elementary construction [40], indirect sum of functions [9] and constructions without extension of the number of variables [11]. Many highly nonlinear Boolean functions can be constructed by using the above constructions.

In this paper, we first present a new secondary construction of bent functions. We show how to construct an $(n+m-2)$-variable bent function from two known bent functions in n variables and in m variables respectively. Furthermore, by selecting the known bent functions as the initial functions of the new secondary construction, we can provide several concrete constructions of bent functions which include primary constructions (Corollary 2 and Corollary 5) and secondary constructions (Corollary 3 and Corollary 4). In

the second part of the paper, we present a generalization of the indirect sum construction for constructing resilient functions with high nonlinearity. On this basis, we provide another two secondary constructions of resilient functions. It is shown that many new $(n+m)$-variable functions with nonlinearity strictly more than $2^{n+m-1}-2^{\lfloor (n+m)/2 \rfloor}$ can be easily obtained by using these secondary constructions, where $\lfloor (n+m)/2 \rfloor$ denotes the largest integer not exceeding $(n+m)/2$.

The rest of the paper is organized as follows. Section 2 introduces basic definitions and cryptographic criteria relevant for Boolean functions. In Section 3, we present a method for constructing bent functions. In Section 4, we provide a generalization of the indirect sum construction for constructing resilient functions. At last, some conclusions are given in Section 5.

2 Preliminaries

In the remainder of this paper, we denote the additions and multiple sums over the finite field $\mathbb{F}_2$ by $\oplus$ and $\bigoplus$. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$, and B_n the set of all n-variable Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. A basic representation of a Boolean function $f(x_1,\ldots,x_n)$ is by the output column of its truth-table, i.e., a binary string of length 2^n,

$$[f(0,\ldots,0,0,0),\ldots,f(1,\ldots,1,1,0),f(1,\ldots,1,1,1)].$$

The *Hamming weight* $\mathrm{wt}(f)$ of a Boolean function $f \in B_n$ is the weight of the above binary string. We say a Boolean function f is *balanced* if its Hamming weight equals 2^{n-1}. The *Hamming distance* $d(f,g)$ between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$.

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form*(ANF):

$$f(x_1,\ldots,x_n)=\bigoplus_{I\subseteq\{1,2,\ldots,n\}} a_I \prod_{l\in I} x_l$$

where $a_I \in \mathbb{F}_2$, and the terms $\prod_{l\in I} x_l$ are called monomials. The *algebraic degree* $\deg(f)$ of a Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its ANF. A Boolean function is affine if it has algebraic degree at most 1. The set of all n-variable affine functions is denoted by A_n. An n-variable affine function with constant term 0 is a linear function, and can be represented as $\omega \cdot x = \omega_1 x_1 \oplus \ldots \oplus \omega_n x_n$ where $\omega=(\omega_1,\ldots,\omega_n) \in \mathbb{F}_2^n, x=(x_1,\ldots,x_n) \in \mathbb{F}_2^n$.

The *nonlinearity* of $f \in B_n$ is its distance to the set of all n-variable affine functions, i.e.,

$$N_f = \min_{g \in A_n} d(f, g).$$

Boolean functions used in cryptographic systems must have high nonlinearity to withstand linear and fast correlation attacks [2].

The *Walsh transform* of $f \in B_n$ is the integer valued function over $\mathbb{F}_2^n$ defined as

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \omega \cdot x}.$$

In terms of Walsh spectrum, the nonlinearity of f is given by

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|.$$

Parseval's equation [26] states that $\sum_{\omega \in \mathbb{F}_2^n} (W_f(\omega))^2 = 2^{2n}$ and implies that

$$N_f \leq 2^{n-1} - 2^{n/2-1}.$$

Definition 1 *[18, 36] A Boolean function $f \in B_n$ is called bent if $W_f(a) = \pm 2^{n/2}$ (that is, $N_f = 2^{n-1} - 2^{n/2-1}$) for every $a \in \mathbb{F}_2^n$ (n even).*

If $f \in B_n$ is bent, then the dual function $\widetilde{f}$ of f, defined on $\mathbb{F}_2^n$ by:

$$W_f(\omega) = 2^{n/2}(-1)^{\widetilde{f}(\omega)}$$

is also bent and its own dual is f itself.

Definition 2 *[47] Let $f \in B_n$. If there exists an even integer r, $0 \leq r \leq n$, such that $\| \{\omega | W_f(\omega) \neq 0, \omega \in \mathbb{F}_2^n\} \| = 2^r$, where $\| \cdot \|$ denotes the size of a set, and $(W_f(\omega))^2$ equals 2^{2n-r} or 0, for every $\omega \in \mathbb{F}_2^n$, then f is called an rth-order plateaued function in n variables. If f is a $2\lceil \frac{n-2}{2} \rceil$th-order plateaued function in n variables, where $\lceil n/2 \rceil$ denotes the smallest integer exceeding $n/2$, then f is also called a semi-bent function.*

A Boolean function $f \in B_n$ is said to be *correlation-immune of order* r ($1 \leq r \leq n$), if the output of f and any r input variables are statistically independent. Balanced rth-order correlation immune functions are called *r-resilient* functions. The set of rth-order correlation immune (resp. r-resilient) Boolean functions is included in that of $(r-1)$th-order correlation immune (resp. $(r-1)$-resilient) Boolean functions. The correlation immunity (resp. resiliency) can also be characterized by using the Walsh transform domain [42]:

Lemma 1 *Let $f \in B_n$, then f is rth-order correlation immune (resp. r-resilient) if and only if its Walsh transform satisfies $W_f(\omega) = 0$, for all $\omega \in F_2^n$ such that $1 \leq \mathrm{wt}(\omega) \leq r$ (resp. $0 \leq \mathrm{wt}(\omega) \leq r$).*

Siegenthaler's Inequality [39] states that any rth-order correlation immune function has degree at most $n - r$, that r-resilient function $(0 \leq r \leq n-1)$ has degree smaller than or equal $n - r - 1$ and that any $(n-1)$-resilient function has algebraic degree 1. Sarkar and Maitra [37] have shown that the nonlinearity of any m-resilient function $(m \leq n-2)$ is divisible by 2^{m+1} and is therefore upper bounded by $2^{n-1} - 2^{m+1}$. If a function achieves this bound (independently obtained by Tarannikov [40] and Zheng and Zhang [48]), then it also achieves Siegenthaler's bound (cf. [40]). More precisely, if f is m-resilient and has algebraic degree d, then its nonlinearity is divisible by $2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$ (see [6, 14]) and can therefore be equal to $2^{n-1}-2^{m+1}$ only if $d = n - m - 1$. Moreover, if an m-resilient function achieves nonlinearity $2^{n-1} - 2^{m+1}$, then the Walsh spectrum of the function has then three values (such functions are often called "plateaued" or "three-valued"). We shall say that an m-resilient function achieves the best possible nonlinearity if its nonlinearity equals $2^{n-1} - 2^{m+1}$. If $2^{n-1} - 2^{m+1}$ is greater than the best possible nonlinearity of all balanced functions (and in particular if it is greater than the best possible nonlinearity $2^{n-1} - 2^{n/2-1}$ of all Boolean functions) then, obviously, a better bound exists. In the case n is even, the best possible nonlinearity of all balanced functions being smaller than $2^{n-1} - 2^{n/2-1}$, we have that $N_f \leq 2^{n-1} - 2^{n/2-1} - 2^{m+1}$ for every m-resilient function f with $m \leq n/2 - 2$. In the case n is odd, N_f is smaller than or equal to the highest multiple of 2^{m+1}, which is less than or equal to the best possible nonlinearity of all Boolean functions. In the sequel, we shall call "Sarkar et al.'s bounds" all these bounds. We shall also extend the definitions of correlation-immune and resilient functions, so that our results are as general as possible: by convention, we shall say that any Boolean function is 0th-order correlation immune and (-1)-resilient and that any balanced function is 0-resilient.

We call (n, m)-functions the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Such function F being given, the Boolean functions $f_1, \ldots, f_m$ defined, at every $x \in \mathbb{F}_2^n$, by $F(x) = (f_1, \ldots, f_m)$, are called the coordinate functions of F. Obviously, these functions include the (single-output) Boolean functions which correspond to the case $m = 1$. Furthermore, for $m = n$, the function $F(x) = (f_1, \ldots, f_n)$ is called a Boolean permutation if $F(x)$ is a bijective mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.

The original Maiorana-McFarland's (M-M) class of bent functions [30]

is the set of all the (bent) Boolean functions on $\mathbb{F}_2^{2n} = \{(x, y), x, y \in \mathbb{F}_2^n\}$ of the form:

$$f(x, y) = x \cdot \phi(y) \oplus g(y)$$

where $\phi(y) = (\phi_1(y), \phi_2(y), \dots, \phi_n(y))$ is any permutation on $\mathbb{F}_2^n$ and $g \in B_n$.

Lemma 2 *For $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^n$, let $\phi_i(y)$, $1 \leq i \leq n$, be an n-variable Boolean function, and $g(y)$ be any n-variable Boolean function. A $2n$-variable Boolean function $f(x, y) = x \cdot \phi(y) \oplus g(y) = \bigoplus_{i=1}^n \phi_i(y_1, \dots, y_n)x_i \oplus g(y_1, \dots, y_n)$ is a bent function if and only if*

$$\phi(y) = (\phi_1(y), \phi_2(y), \dots, \phi_n(y))$$

is a Boolean permutation.

This property comes directly from the fact that any restriction of f obtained by fixing y is affine. We shall say that the coordinates of x are "affine". In the next section, we shall use such functions in a different - but equivalent - form: n will be the global number of variables (instead of $2n$) and the "affine" variables will be $x_1, \dots, x_{n/2}$, that is, the functions will have the form $f(x_1, \dots, x_n) = \bigoplus_{i=1}^{n/2} \phi_i(x_{n/2+1}, \dots, x_n)\, x_i \oplus g(x_{n/2+1}, \dots, x_n)$.

3 Secondary constructions of bent functions

In this section, we present secondary constructions of bent functions. Before that, we first recall the concept of complementary plateaued functions. It will play an important role in the following constructions.

Definition 3 *[47] Let p be a positive odd number and $g_1, g_2 \in B_p$. Then g_1 and g_2 are said to be complementary $(p-1)$th-order plateaued functions in p variables if they are p-variable $(p-1)$th-order plateaued functions, and satisfy the property that $W_{g_1}(\omega) = 0$ if and only if $W_{g_2}(\omega) \neq 0$.*

Lemma 3 *[47] Let n be a positive even number and $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$. Then $f(x)$ is bent if and only if the two functions, $f(x_1, \dots, x_{j-1}, 0, x_{j+1}, \dots, x_n)$ and $f(x_1, \dots, x_{j-1}, 1, x_{j+1}, \dots, x_n)$ are complementary $(n-2)$th-order plateaued functions in $n-1$ variables, where $j = 1, 2, \dots, n$.*

In [9], Carlet designed a secondary construction of bent functions, often called the *indirect sum*:

Corollary 1 *[9, 12] Let $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$. Let f_1 and f_2 be two n-variable bent functions (n even) and let g_1 and g_2 be two m-variable bent functions (m even). Define*

$$h(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)\,(g_1 \oplus g_2)(y).$$

Then h is bent and its dual is obtained from $\widetilde{f_1}, \widetilde{f_2}, \widetilde{g_1}$ and $\widetilde{g_2}$ by the same formula as h is obtained from f_1, f_2, g_1 and g_2.

This above secondary construction was altered into constructions of resilient functions, see [9], which includes as a particular case the well-know *direct sum* [39], that we recall: for $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$, let $f(x)$ be an n-variable t-resilient function ($t \geq 0$) and $g(y)$ be an m-variable k-resilient function ($k \geq 0$), then the function

$$h(x,y) = f(x) \oplus g(y)$$

is a $(t+k+1)$-resilient function in $n+m$ variables. The nonlinearity of $h(x,y)$ is equal to $2^n N_g + 2^m N_f - 2N_f N_g$.

In the present paper, we first modify the indirect sum into a new construction of bent functions:

Construction 1 *Let n and m be two positive even numbers. For $X = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $Y = (y_1, \ldots, y_m) \in \mathbb{F}_2^m$, $x = (x_1, \ldots, x_{\mu-1}, x_{\mu+1}, \ldots, x_n) \in \mathbb{F}_2^{n-1}$, $y = (y_1, \ldots, y_{\rho-1}, y_{\rho+1}, \ldots, y_m) \in \mathbb{F}_2^{m-1}$, let $f(X)$ be an n-variable bent function and $g(Y)$ an m-variable bent function. We consider the restrictions of f equal to $f_0(x) = f(x_1, \ldots, x_{\mu-1}, 0, x_{\mu+1}, \ldots, x_n)$, $f_1(x) = f(x_1, \ldots, x_{\mu-1}, 1, x_{\mu+1}, \ldots, x_n)$ and of g equal to $g_0(y) = g(y_1, \ldots, y_{\rho-1}, 0, y_{\rho+1}, \ldots, y_m)$, $g_1(y) = g(y_1, \ldots, y_{\rho-1}, 1, y_{\rho+1}, \ldots, y_m)$, where $\mu \in \{1, 2, \ldots, n\}$, $\rho \in \{1, 2, \ldots, m\}$ and we define:*

$$h(x,y) = f_0(x) \oplus g_0(y) \oplus (f_0 \oplus f_1)(x)\,(g_0 \oplus g_1)(y).$$

This construction indeed provides bent functions:

Theorem 1 *Let $f(X) \in B_n, g(Y) \in B_m$ and $h(x,y) \in B_{n+m-2}$ be defined as in Construction 1. Then h is a bent function in $n+m-2$ variables. Further, the dual of h is obtained from $\overline{f_0}(x) = \widetilde{f}(x_1, \ldots, x_{\mu-1}, 0, x_{\mu+1}, \ldots, x_n)$, $\overline{f_1}(x) = \widetilde{f}(x_1, \ldots, x_{\mu-1}, 1, x_{\mu+1}, \ldots, x_n)$, $\overline{g_0}(y) = \widetilde{g}(y_1, \ldots, y_{\rho-1}, 0, y_{\rho+1}, \ldots, y_m)$ and $\overline{g_1}(y) = \widetilde{g}(y_1, \ldots, y_{\rho-1}, 1, y_{\rho+1}, \ldots, y_m)$, by the same formula as h is obtained from f_0, f_1, g_0 and g_1.*

Proof. According to Definition 1, the bentness of $h(x,y)$ will be proved if we can show that $W_h(a,b) = \pm 2^{(n+m-2)/2}$ for every $a = (a_1, \ldots, a_{\mu-1}, a_{\mu+1}, \ldots, a_n) \in \mathbb{F}_2^{n-1}$ and $b = (b_1, \ldots, b_{\rho-1}, b_{\rho+1}, \ldots, b_m) \in \mathbb{F}_2^{m-1}$. As shown in [9] for all Boolean functions, we have:

$$\begin{aligned}
W_h(a,b) &= \sum_{x\in\mathbb{F}_2^{n-1}} \sum_{y\in\mathbb{F}_2^{m-1}} (-1)^{h(x,y)\oplus a\cdot x\oplus b\cdot y} \\
&= \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ f_0\oplus f_1=0}} \sum_{y\in\mathbb{F}_2^{m-1}} (-1)^{f_0(x)\oplus a\cdot x}(-1)^{g_0(y)\oplus b\cdot y} \\
&+ \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ f_0\oplus f_1=1}} \sum_{y\in\mathbb{F}_2^{m-1}} (-1)^{f_0(x)\oplus a\cdot x}(-1)^{g_1(y)\oplus b\cdot y} \\
&= W_{g_0}(b) \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ f_0\oplus f_1=0}} (-1)^{f_0(x)\oplus a\cdot x} + W_{g_1}(b) \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ f_0\oplus f_1=1}} (-1)^{f_0(x)\oplus a\cdot x} \qquad (1)\\
&= W_{g_0}(b) \sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{f_0(x)\oplus a\cdot x} \left(\frac{1+(-1)^{(f_0\oplus f_1)(x)}}{2}\right) \\
&+ W_{g_1}(b) \sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{f_0(x)\oplus a\cdot x} \left(\frac{1-(-1)^{(f_0\oplus f_1)(x)}}{2}\right) \\
&= \frac{1}{2}W_{g_0}(b)\left[W_{f_0}(a)+W_{f_1}(a)\right] + \frac{1}{2}W_{g_1}(b)\left[W_{f_0}(a)-W_{f_1}(a)\right].
\end{aligned}$$

From Lemma 3, f_0 and f_1 are complementary $(n-2)$th-order plateaued functions in $n-1$ variables, g_0 and g_1 are complementary $(m-2)$th-order plateaued functions in $m-1$ variables. According to Definition 3 and Definition 2, it follows that $W_h(a,b) = \pm 2^{(n+m-2)/2}$ for every $a \in \mathbb{F}_2^{n-1}, b \in \mathbb{F}_2^{m-1}$.

Next, we show that the dual of h is obtained from $\overline{f_0}, \overline{f_1}, \overline{g_0}$ and $\overline{g_1}$. We have:

$$\begin{aligned}
&W_f(a_1, \ldots, a_{\mu-1}, 0, a_{\mu+1}, \ldots, a_n) \\
&= 2^{\frac{n}{2}}(-1)^{\overline{f_0}(a)} \\
&= \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ x_\mu=0}} (-1)^{f_0(x)\oplus a\cdot x} + \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ x_\mu=1}} (-1)^{f_1(x)\oplus a\cdot x} \qquad (2)\\
&= W_{f_0}(a) + W_{f_1}(a).
\end{aligned}$$

Further,

$$\begin{aligned}
&W_f(a_1, \ldots, a_{\mu-1}, 1, a_{\mu+1}, \ldots, a_n) \\
&= 2^{\frac{n}{2}}(-1)^{\overline{f_1}(a)} \\
&= \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ x_\mu=0}} (-1)^{f_0(x)\oplus a\cdot x} - \sum_{\substack{x\in\mathbb{F}_2^{n-1}\\ x_\mu=1}} (-1)^{f_1(x)\oplus a\cdot x} \qquad (3)\\
&= W_{f_0}(a) - W_{f_1}(a).
\end{aligned}$$

Combining Relations (1), (2) and (3), we have

$$\begin{aligned} W_h(a,b) &= 2^{\frac{n+m}{2}-2}\left((-1)^{\overline{g_0}(b)} + (-1)^{\overline{g_1}(b)}\right)(-1)^{\overline{f_0}(a)} \\ &+2^{\frac{n+m}{2}-2}\left((-1)^{\overline{g_0}(b)} - (-1)^{\overline{g_1}(b)}\right)(-1)^{\overline{f_1}(a)} \\ &= 2^{\frac{n+m}{2}-1}(-1)^{\widetilde{h}(a,b)}. \end{aligned}$$

According to the above equality, it follows that

$$\begin{aligned} (-1)^{\widetilde{h}(a,b)} &= \tfrac{1}{2}\left((-1)^{\overline{g_0}(b)} + (-1)^{\overline{g_1}(b)}\right)(-1)^{\overline{f_0}(a)} \\ &+\tfrac{1}{2}\left((-1)^{\overline{g_0}(b)} - (-1)^{\overline{g_1}(b)}\right)(-1)^{\overline{f_1}(a)}. \end{aligned}$$

Then we have

$$\widetilde{h}(a,b) = \overline{g_0}(b) \oplus \overline{f_0}(a) \oplus (\overline{g_0}(b) \oplus \overline{g_1}(b))\left(\overline{f_0}(a) \oplus \overline{f_1}(a)\right).$$

That is,

$$\widetilde{h}(x,y) = \overline{g_0}(y) \oplus \overline{f_0}(x) \oplus (\overline{g_0}(y) \oplus \overline{g_1}(y))\left(\overline{f_0}(x) \oplus \overline{f_1}(x)\right).$$

Remark 1 Without loss of generality (up to linear equivalence) let us take $\mu = \rho = n$. Let us denote $e = (0, \ldots, 0, 1)$. For any x and y, we have $(g_0 \oplus g_1)(y) = D_e g(y, 0)$ where "," denotes concatenation et $D_e g$ is the derivative of g, defined as $D_e g(y, 0) = g(y, 0) \oplus g(y, 1)$. Then $h(x, y) = f(x, 0) \oplus g(y, 0)$ if $D_e g(y, 0) = 0$ and $h(x, y) = f(x, 1) \oplus g(y, 0)$ if $D_e g(y, 0) = 1$. Hence, $h(x, y) = f(x, 0) \oplus g(y, 0) \oplus D_e f(x, 0) D_e g(y, 0) = f(x, D_e g(y, 0)) \oplus g(y, 0) = f(x, 0) \oplus g(y, D_e f(x, 0)$. The derivative plays a role in a construction from [15] (which has been generalized in [11]), but the present construction is clearly different since it builds $(n+m-2)$-variable functions from n-variable and m-variable ones.

Remark 2 Taking $h(x, y) = f_1(x) \oplus g_0(y) \oplus (f_0 \oplus f_1)(x)\,(g_0 \oplus g_1)(y)$ or $h(x, y) = f_0(x) \oplus g_1(y) \oplus (f_0 \oplus f_1)(x)\,(g_0 \oplus g_1)(y)$ or $h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_0 \oplus f_1)(x)\,(g_0 \oplus g_1)(y)$ gives three other bent functions; of course these functions correspond to applying Construction 1 to functions affinely equivalent to f and g.

In what follows, we analyze the properties of $h(x, y)$. Before that, we first introduce a notation. *The algebraic degree of variable x_i in f*, denoted by $\deg(f, x_i)$, is the number of variables in the longest term of f that contains x_i.

Proposition 1 *Let n (>2) and m (>2) be two even numbers. Let $f(X) \in B_n, g(Y) \in B_m$ and $h(x,y) \in B_{n+m-2}$ be defined as in Construction 1. Then $2 \leq \deg(h) \leq \frac{n+m-2}{2} - 1$.*

Proof. Clearly, $2 \leq \deg(h)$ since h is bent. If $\deg(f) = 2$ and $\deg(g) = 2$, then $\deg(h) = 2$.
According to the bentness of $f(X)$ (resp. $g(Y)$), we have $\deg(f) \leq n/2$ (resp. $\deg(g) \leq m/2$). Further, we have $\deg(f_0 \oplus f_1) \leq n/2 - 1$ (resp. $\deg(g_0 \oplus g_1) \leq m/2 - 1$) because $\deg(f(x) \oplus f(x \oplus a) \leq n/2 - 1$, where $a \in \mathbb{F}_2^n$. Thus, from Construction 1, we have $\deg(h) \leq \frac{n+m-2}{2} - 1$, the equality holds if and only if $\deg(f, x_\mu) = n/2$ and $\deg(g, y_\rho) = m/2$.

Remark 3 If $m = 2$, then $g(Y) = y_1y_2 \oplus l(y_1, y_2)$, where $l(y_1, y_2)$ is an affine function. By Construction 1, we have $\deg(f_0) \leq \deg(h) \leq \deg(f) \leq (n+m-2)/2$. From Proposition 1, the $(n+m-2)$-variable functions constructed by Construction 1 have algebraic degree not exceeding $(n+m-2)/2-1$ if $n > 2$ and $m > 2$. Thus, they can not belong to the PS^- class, since all n-variable functions in PS^- have algebraic degree $n/2$ exactly [18]. In addition, the constructed function h has algebraic degree 2 if and only if both f and g have algebraic degree 2.

Let us apply Construction 1 to M-M functions $f(x) = \bigoplus_{i=1}^{n/2} \phi_i(x_{n/2+1}, \ldots, x_n)x_i \oplus u(x_{n/2+1}, \ldots, x_n)$ and $g(y) = \bigoplus_{j=1}^{m/2} \psi_j(y_{m/2+1}, \ldots, y_m)y_i \oplus v(y_{m/2+1}, \ldots, y_m)$, where $u(x_{n/2+1}, \ldots, x_n)$ is any Boolean function in $n/2$ variables and $v(y_{m/2+1}, \ldots, y_m)$ is any Boolean function in $m/2$ variables. We deduce the following primary construction:

Corollary 2 *Let n and m be two positive even numbers and $\mu \in \{1, \ldots, n/2\}$, $\rho \in \{1, \ldots, m/2\}$. For $x = (x_1, \ldots, x_{\mu-1}, x_{\mu+1}, \ldots, x_n) \in \mathbb{F}_2^{n-1}, y = (y_1, \ldots, y_{\rho-1}, y_{\rho+1}, \ldots, y_m) \in \mathbb{F}_2^{m-1}$, let $\phi(x_{n/2+1}, \ldots, x_n) = \big(\phi_1, \ldots, \phi_{n/2}\big)$ be a Boolean permutation in $n/2$ variables and $\psi(y_{m/2+1}, \ldots, y_m) = \big(\psi_1, \ldots, \psi_{m/2}\big)$ a Boolean permutation in $m/2$ variables. Then the $(n+m-2)$-variable function*

$$\begin{aligned} h(x,y) &= \bigoplus_{\substack{i=1 \\ i\neq\mu}}^{n/2} \phi_i(x_{n/2+1}, \ldots, x_n)\, x_i \oplus \bigoplus_{\substack{j=1 \\ j\neq\rho}}^{m/2} \psi_j(y_{1+m/2}, \ldots, y_m)\, y_j \\ &\oplus \phi_\mu(x_{n/2+1}, \ldots, x_n)\psi_\rho(y_{1+m/2}, \ldots, y_m) \\ &\oplus u(x_{n/2+1}, \ldots, x_n) \oplus v(y_{1+m/2}, \ldots, y_m) \end{aligned} \tag{4}$$

is bent, where $u(x_{n/2+1}, \ldots, x_n) \in B_{n/2}, v(y_{m/2+1}, \ldots, y_m) \in B_{m/2}$.

Remark 4 The bent functions given by Corollary 2, have a form similar to those of M-M functions; indeed, $\phi_\mu(x_{n/2+1},\dots,x_n)\psi_\rho(y_{m/2+1},\dots,y_m)$ does not depend on the "affine" variables. There are cases where $h(x,y)$ is an $(n+m-2)$-variable M-M bent function; for instance when $\phi_\mu = x_l$ and $\big(\phi_1,\dots,\phi_{\mu-1},\phi_{\mu+1},\phi_{n/2}\big)$ is a Boolean permutation in $n/2-1$ variables, or $\psi_\rho = y_t$ and $(\psi_1,\dots,\ \psi_{\rho-1},\psi_{\rho+1},\psi_{m/2}\big)$ is a Boolean permutation in $m/2-1$ variables. But the functions of Corollary 2 are in general not M-M functions; the mapping:

$$\begin{gathered}\Theta : (x_{n/2+1},\dots,x_n,y_{m/2+1},\dots,y_m) \mapsto \\ \big(\phi_1(x_{n/2+1},\dots,x_n),\dots,\phi_{\mu-1}(x_{n/2+1},\dots,x_n), \\ \phi_{\mu+1}(x_{n/2+1},\dots,x_n),\dots,\phi_{n/2}(x_{n/2+1},\dots,x_n), \\ \psi_1(y_{m/2+1},\dots,y_m),\dots,\psi_{\rho-1}(y_{m/2+1},\dots,y_m), \\ \psi_{\rho+1}(y_{m/2+1},\dots,y_m),\dots,\psi_{m/2}(y_{m/2+1},\dots,y_m)\big)\end{gathered}$$

is not a permutation; it is even not a vectorial function with an equal number of input and output bits.

In [8, Proposition 1] is introduced a generalization of the M-M construction: let $s \geq r$ and let Θ be any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$ such that, for every $a \in \mathbb{F}_2^r$, the set $\Theta^{-1}(a)$ is an $(n-2r)$-dimensional affine subspace of $\mathbb{F}_2^s$ and let g be any Boolean function on $\mathbb{F}_2^s$ whose restriction to $\Theta^{-1}(a)$ is bent for every $a \in \mathbb{F}_2^r$, if $n > 2r$ (no condition on g being imposed if $n = 2r$, which corresponds to the original M-M construction), then $x \cdot \Theta(y) \oplus g(y)$ is bent. We can see that Corollary 2 is in some cases a particular case of this general construction of bent functions with $s = (m+n)/2, r = (m+n-4)/2$ (this happens for instance when Θ is an affine mapping). But, in general, it is not, since the condition "$\Theta^{-1}(a)$ is an $(n-2r)$-dimensional affine subspace of $\mathbb{F}_2^s$" is not satisfied.

According to Remark 2 and Corollary 2, we know that $h(x,y)\oplus\phi_\mu(x_{n/2+1},\dots,x_n)$, $h(x,y)\oplus\psi_\rho(y_{m/2+1},\dots,y_m)$ and $h(x,y)\oplus\phi_\mu(x_{n/2+1},\dots,x_n)\oplus\psi_\rho(y_{m/2+1},\dots,y_m)$ are also bent functions, where $h(x,y)$ are defined as Corollary 2. Further, similarly to Corollary 2, we are able to select $\mu \in \{1,\dots,n/2\}$, $\rho \in \{\frac{m}{2}+1,\dots,m\}$ or $\mu \in \{\frac{n}{2}+1,\dots,n\}$, $\rho \in \{1,\dots,m/2\}$ or $\mu \in \{\frac{n}{2}+1,\dots,n\}$, $\rho \in \{\frac{m}{2}+1,\dots,m\}$. This gives three primary constructions similar to that of Corollary 2. We can also apply Construction 1 using as initial functions two elements of the PS_{ap} class of bent functions (introduced in [18] and recalled for instance in [12]). Recall that the functions of this class are defined over $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \sim \mathbb{F}_2^n$ as $f(x,y) =$

$g(x/y)$ where $x, y \in \mathbb{F}_{2^{n/2}}$ and g is balanced on $\mathbb{F}_{2^{n/2}}$, with the convention $x/0 = 0$. To define f_0 we need to restrict f to a linear hyperplane $\{(x,y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \,|\, Tr_1^{n/2}(ax \oplus by) = 0\}$ of $\mathbb{F}_2^n$, where $Tr_1^{n/2}$ is the absolute trace over $\mathbb{F}_{2^{n/2}}$ and $(a,b) \neq (0,0)$. We have $(f_0 \oplus f_1)(x,y) = D_{(\alpha,\beta)} f(x,y)$ for some $(\alpha, \beta) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ such that $tr(a\alpha + b\beta) = 1$.

Corollary 3 *Let n and m be two positive even numbers. We identify $\mathbb{F}_2^{n/2}$ (resp. $\mathbb{F}_2^{m/2}$) with the Galois field $\mathbb{F}_{2^{n/2}}$ (resp. $\mathbb{F}_{2^{m/2}}$). Let θ (resp. ϑ) be a balanced function on $\mathbb{F}_{2^{n/2}}$ (resp. $\mathbb{F}_{2^{m/2}}$). Let $(x,y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, $(z,\tau) \in \mathbb{F}_{2^{m/2}} \times \mathbb{F}_{2^{m/2}}$, let $f(x,y) = \theta(\frac{x}{y})$ for $y \neq 0$, otherwise $f(x,y) = 0$, let $g(z,\tau) = \theta(\frac{z}{\tau})$ for $\tau \neq 0$, otherwise $g(z,\tau) = 0$. Let $f_0(x,y)$ (resp. $g_0(z,\tau)$) be the restriction of f (resp. g) on $\{(x,y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} | Tr_1^{n/2}(ax \oplus by) = 0\}$ (resp. $\{(z,\tau) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{m/2}} | Tr_1^{m/2}(cz \oplus d\tau) = 0\}$), where $(a,b) \neq (0,0) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, $(c,d) \neq (0,0) \in \mathbb{F}_{2^{m/2}} \times \mathbb{F}_{2^{m/2}}$. We take $f_1(x,y) = f_0(x \oplus \alpha, y \oplus \beta)$, where $Tr_1^{n/2}(a\alpha \oplus b\beta) = 1, (\alpha,\beta) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ and $g_1(z,\tau) = g_0(z \oplus u, \tau \oplus v)$, where $Tr_1^{m/2}(cu \oplus dv) = 1, (u,v) \in \mathbb{F}_{2^{m/2}} \times \mathbb{F}_{2^{m/2}}$. Then*

$$h(x,y,z,\tau) = f_0(x,y) \oplus g_0(z,\tau) \oplus (f_0 \oplus f_1)(x,y)\,(g_0 \oplus g_1)(z,\tau)$$

is a bent function on $\mathbb{F}_{2^{n+m-2}}$.

Of course we could also apply Construction 1 using as initial functions an M-M function and a function of PS_{ap}.

In 1976, Rothaus presented a secondary construction which uses three initial n-variable bent functions $f^{(1)}, f^{(2)}, f^{(3)}$ to build a fourth one f which is an $(n+2)$-variable bent function:

Rothaus' construction [36]: Let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ and $x_{n+1}, x_{n+2} \in \mathbb{F}_2$. Let $f^{(1)}(x)$, $f^{(2)}(x)$, $f^{(3)}(x)$ be bent functions on $\mathbb{F}_2^n$ such that $f^{(1)}(x) \oplus f^{(2)}(x) \oplus f^{(3)}(x)$ is bent as well, then the function defined at every element $(x, x_{n+1}, x_{n+2}) \in \mathbb{F}_2^{n+2}$ by:

$$\begin{aligned} f(x, x_{n+1}, x_{n+2}) &= f^{(1)}(x)f^{(2)}(x) \oplus f^{(1)}(x)f^{(3)}(x) \\ &\oplus f^{(2)}(x)f^{(3)}(x) \oplus [f^{(1)}(x) \oplus f^{(2)}(x)]x_{n+1} \\ &\oplus [f^{(1)}(x) \oplus f^{(3)}(x)]x_{n+2} \oplus x_{n+1}x_{n+2} \end{aligned}$$

is a bent function in $n+2$ variables.

We apply Construction 1 to bent functions constructed by Rothaus' construction.

Corollary 4 *Let n and m be two positive even numbers and $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m$, $x_{n+1}, x_{n+2}, y_{m+1}, y_{m+2} \in \mathbb{F}_2$. Let an $(n+2)$-variable bent function f and an $(m+2)$-variable bent function g be built by means of Rothaus' construction, respectively from n-variable bent functions $f^{(1)}, f^{(2)}, f^{(3)}$ and m-variable bent functions $g^{(1)}, g^{(2)}, g^{(3)}$. Then*

$$\begin{aligned} h(x,y,x_{n+1},y_{m+1}) \; &= f^{(1)}(x)f^{(2)}(x) \oplus f^{(1)}(x)f^{(3)}(x) \\ &\oplus f^{(2)}(x)f^{(3)}(x) \oplus g^{(1)}(y)g^{(2)}(y) \\ &\oplus g^{(1)}(y)g^{(3)}(y) \oplus g^{(2)}(y)g^{(3)}(y) \\ &\oplus [f^{(1)}(x) \oplus f^{(2)}(x)]x_{n+1} \\ &\oplus [g^{(1)}(y) \oplus g^{(2)}(y)]y_{m+1} \\ &\oplus [f^{(1)}(x) \oplus f^{(3)}(x)][g^{(1)}(y) \oplus g^{(3)}(y)] \\ &\oplus [f^{(1)}(x) \oplus f^{(3)}(x)]y_{m+1} \\ &\oplus [g^{(1)}(y) \oplus g^{(3)}(y)]x_{n+1} \\ &\oplus x_{n+1}y_{m+1}. \end{aligned} \tag{5}$$

is a bent function in $n+m+2$ variables.

Proof. We select f and g as the initial functions of Construction 1 and set $\mu = n+2, \rho = m+2$. From Theorem 1, we know that $h(x,y,x_{n+1},y_{m+1})$ is a bent function in $n+m+2$ variables.

Next, we consider the bent functions in class D as the initial functions of Construction 1. We first introduce class D, which has been derived in [3] from M-M bent functions, by adding to some functions of this class the indicators of some vector subspaces:

The class D of all the functions of the form $\bigoplus_{i=1}^{n/2} \phi_i(x_{n/2+1}, \ldots, x_n)x_i \oplus 1_{E_1}(x_1, \ldots, x_{n/2})1_{E_2}(x_{n/2+1}, \ldots, x_n)$, where ϕ is any permutation on $\mathbb{F}_2^{n/2}$, E_1, E_2 are two linear subspaces of $\mathbb{F}_2^{n/2}$ such that $\phi(E_2) = E_1^{\perp}$ and $1_{E_1}(x_1, \ldots, x_{n/2})$ (resp. $1_{E_2}(x_{n/2+1}, \ldots, x_n)$ is the characteristic function of E_1 (resp. E_2).

Corollary 5 *Let n and m be two positive even numbers and $\mu \in \{1, \ldots, n/2\}$, $\rho \in \{1, \ldots, m/2\}$. For $x = (x_1, \ldots, x_{\mu-1}, x_{\mu+1}, \ldots, x_n) \in \mathbb{F}_2^{n-1}, y = (y_1, \ldots, y_{\rho-1}, y_{\rho+1}, \ldots, y_m) \in \mathbb{F}_2^{m-1}$, let $\phi(X_1^{(n/2)}) = \big(\phi_1, \ldots, \phi_{n/2}\big)$ be a Boolean permutation in $\frac{n}{2}$ variables and $\psi(Y_1^{(m/2)}) = \big(\psi_1, \ldots, \psi_{m/2}\big)$ a Boolean permutation in $\frac{m}{2}$ variables, where $X_1^{(n/2)} = (x_{n/2+1}, \ldots, x_n)$, $Y_1^{(m/2)} = (y_{m/2+1}, \ldots, y_m)$. Let E_1, E_2 (resp. Ξ_1, Ξ_2) be two linear subspaces of $\mathbb{F}_2^{n/2}$ (resp. $\mathbb{F}_2^{m/2}$) such that $\phi(E_2) = E_1^{\perp}$ (resp. $\psi(\Xi_2) = \Xi_1^{\perp}$). Then the $(n+m-2)$-variable*

function

$$
\begin{aligned}
h(x,y) = {} & \bigoplus_{\substack{i=1\\ i\neq\mu}}^{n/2} \phi_i(X_1^{(n/2)})\, x_i \oplus \bigoplus_{\substack{j=1\\ j\neq\rho}}^{m/2} \psi_j(Y_1^{(m/2)})\, y_j \\
& \oplus \bigoplus_{\tau\in E_1} (\tau_\mu \oplus 1) \prod_{\substack{i=1\\ i\neq\mu}}^{n/2} (x_i \oplus \tau_i \oplus 1) 1_{E_2}(X_1^{(n/2)}) \\
& \oplus \bigoplus_{\varsigma\in \Xi_1} (\varsigma_\rho \oplus 1) \prod_{\substack{j=1\\ j\neq\rho}}^{m/2} (y_j \oplus \varsigma_j \oplus 1) 1_{\Xi_2}(Y_1^{(m/2)}) \\
& \oplus \phi_\mu(X_1^{(n/2)})\psi_\rho(Y_1^{(m/2)}) \\
& \oplus \psi_\rho(Y_1^{(m/2)}) \left(\bigoplus_{\tau\in E_1} \prod_{\substack{i=1\\ i\neq\mu}}^{n/2} (x_i \oplus \tau_i \oplus 1) \right) 1_{E_2}(X_1^{(n/2)}) \\
& \oplus \phi_\mu(X_1^{(n/2)}) \left(\bigoplus_{\varsigma\in \Xi_1} \prod_{\substack{j=1\\ j\neq\rho}}^{m/2} (y_j \oplus \varsigma_j \oplus 1) \right) 1_{\Xi_2}(Y_1^{(m/2)}) \\
& \oplus \left(\bigoplus_{\tau\in E_1} \prod_{\substack{i=1\\ i\neq\mu}}^{n/2} (x_i \oplus \tau_i \oplus 1) \right) 1_{E_2}(X_1^{(n/2)}) \\
& \times \left(\bigoplus_{\varsigma\in \Xi_1} \prod_{\substack{j=1\\ j\neq\rho}}^{m/2} (y_j \oplus \varsigma_j \oplus 1) \right) 1_{\Xi_2}(Y_1^{(m/2)}).
\end{aligned}
$$

is bent.

Proof. Let $f = \bigoplus_{i=1}^{n/2} \phi_i(X_1^{(n/2)})\, x_i \oplus 1_{E_1}(x_1, \ldots, x_{n/2}) 1_{E_2}(X_1^{(n/2)})$, $g = \bigoplus_{j=1}^{m/2} \psi_j(Y_1^{(m/2)})\, y_j \oplus 1_{\Xi_1}(y_1, \ldots, y_{m/2}) 1_{\Xi_2}(Y_1^{(m/2)})$. Clearly, $h(x,y)$ is a bent function in $n+m-2$ variables if we select f and g as the initial functions of Construction 1.

4 Secondary constructions of highly nonlinear functions

In this section, we present a generalization of the indirect sum construction for constructing resilient functions with high nonlinearity. Before that, we first recall the secondary construction of bent functions deduced by Carlet, Zhang and Hu in [16].

Lemma 4 *Let n and m be two even positive integers. Let $f_1(x), f_2(x)$ and $f_3(x)$ be bent functions in n variables. Let $g_1(y), g_2(y)$ and $g_3(y)$ be bent functions in m variables. Denote by ν_1 the function $f_1 \oplus f_2 \oplus f_3$ and by ν_2 the function $g_1 \oplus g_2 \oplus g_3$. If both ν_1 and ν_2 are bent functions and if $\widetilde{\nu_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, then*

$$f(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y) \oplus (f_2 \oplus f_3)(x)(g_2 \oplus g_3)(y)$$

is a bent function in $n+m$ variables.

Now, we adapt the above construction for constructing resilient functions.

Theorem 2 *Let n, m, t and k be four integers such that $-1 \leq t < n$ and $-1 \leq k < m$. Let $f_1(x), f_2(x)$ and $f_3(x)$ be three t-resilient functions in n variables. Let $g_1(y), g_2(y)$ and $g_3(y)$ be k-resilient functions in m variables. If $f_1(x) \oplus f_2(x) \oplus f_3(x)$ is also a t-resilient function in n variables and $g_1(y) \oplus g_2(y) \oplus g_3(y)$ is also an r-resilient function in m variables, then the function*

$$f(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y) \oplus (f_2 \oplus f_3)(x)(g_2 \oplus g_3)(y)$$

is a $(t+k+1)$-resilient function in $n+m$ variables.

Proof. From Lemma 1, $f(x,y)$ is a $(t+k+1)$-resilient function in $n+m$ variables if we can prove that $W_f(\alpha,\beta)$ is null for every $\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^m$ such that $0 \leq wt(\alpha,\beta) \leq t+k+1$. We have:

$$\begin{aligned}
& W_f(\alpha,\beta) \\
&= \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^m} (-1)^{f(x,y)\oplus\alpha\cdot x\oplus\beta\cdot y} \\
&= \sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)=f_2(x)=f_3(x)=0}} (-1)^{\alpha\cdot x} \sum_{y\in\mathbb{F}_2^m} (-1)^{g_1(y)\oplus\beta\cdot y} \\
&+ \sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)=f_2(x)=f_3(x)=1}} (-1)^{1\oplus\alpha\cdot x} \sum_{y\in\mathbb{F}_2^m} (-1)^{g_1(y)\oplus\beta\cdot y} \\
&+ \sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)\neq f_2(x)=f_3(x)=0}} (-1)^{1\oplus\alpha\cdot x} \sum_{y\in\mathbb{F}_2^m} (-1)^{g_2(y)\oplus\beta\cdot y} \qquad (6)\\
&+ \sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)\neq f_2(x)=f_3(x)=1}} (-1)^{\alpha\cdot x} \sum_{y\in\mathbb{F}_2^m} (-1)^{g_2(y)\oplus\beta\cdot y} \\
&+ \sum_{\substack{x\in\mathbb{F}_2^n,\\ f_2(x)\neq f_1(x)=f_3(x)=0}} (-1)^{\alpha\cdot x} \sum_{y\in\mathbb{F}_2^m} (-1)^{g_3(y)\oplus\beta\cdot y}
\end{aligned}$$

$$+\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_2(x)\neq f_1(x)=f_3(x)=1}}(-1)^{1\oplus\alpha\cdot x}\sum_{y\in\mathbb{F}_2^m}(-1)^{g_3(y)\oplus\beta\cdot y}$$
$$+\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_3(x)\neq f_1(x)=f_2(x)=0}}(-1)^{\alpha\cdot x}\sum_{y\in\mathbb{F}_2^m}(-1)^{g_1(y)\oplus g_2(y)\oplus g_3(y)\oplus\beta\cdot y}$$
$$+\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_3(x)\neq f_1(x)=f_2(x)=1}}(-1)^{1\oplus\alpha\cdot x}\sum_{y\in\mathbb{F}_2^m}(-1)^{g_1(y)\oplus g_2(y)\oplus g_3(y)\oplus\beta\cdot y}$$
$$=W_{g_1}(\beta)\left[\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)=f_2(x)=f_3(x)=0}}(-1)^{\alpha\cdot x}-\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)=f_2(x)=f_3(x)=1}}(-1)^{\alpha\cdot x}\right]$$
$$+W_{g_2}(\beta)\left[\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)\neq f_2(x)=f_3(x)=1}}(-1)^{\alpha\cdot x}-\sum_{\substack{x\in\mathbb{F}_2^n,\\ f_1(x)\neq f_2(x)=f_3(x)=0}}(-1)^{\alpha\cdot x}\right]$$
$$+W_{g_3}(\beta)\left[\sum_{\substack{x\in\mathbb{F}_2^n\\ f_2(x)\neq f_1(x)=f_3(x)=0}}(-1)^{\alpha\cdot x}-\sum_{\substack{x\in\mathbb{F}_2^n\\ f_2(x)\neq f_1(x)=f_3(x)=1}}(-1)^{\alpha\cdot x}\right]$$
$$+W_{g_1\oplus g_2\oplus g_3}(\beta)\left[\sum_{\substack{x\in\mathbb{F}_2^n\\ f_1(x)=f_2(x)=0\\ f_3(x)=1}}(-1)^{\alpha\cdot x}-\sum_{\substack{x\in\mathbb{F}_2^n\\ f_1(x)=f_2(x)=1\\ f_3(x)=0}}(-1)^{\alpha\cdot x}\right]$$
$$=W_{g_1}(\beta)\left[\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1+(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_3(x)}}{2}\right)-\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1-(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_3(x)}}{2}\right)\right]$$
$$+W_{g_2}(\beta)\left[\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1+(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_3(x)}}{2}\right)-\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1-(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_3(x)}}{2}\right)\right]$$
$$+W_{g_3}(\beta)\left[\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1+(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_3(x)}}{2}\right)-\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1-(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_3(x)}}{2}\right)\right]$$
$$+W_{g_1\oplus g_2\oplus g_3}(\beta)\left[\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1+(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_3(x)}}{2}\right)-\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x}\left(\tfrac{1-(-1)^{f_1(x)}}{2}\right)\left(\tfrac{1-(-1)^{f_2(x)}}{2}\right)\left(\tfrac{1+(-1)^{f_3(x)}}{2}\right)\right]$$

Hence:

$$\begin{aligned} W_f(\alpha,\beta) = & \tfrac{1}{4}W_{g_1}(\beta)\left[W_{f_1}(\alpha)+W_{f_2}(\alpha)\ +W_{f_3}(\alpha)+W_{f_1\oplus f_2\oplus f_3}(\alpha)\right] \\ & +\tfrac{1}{4}W_{g_2}(\beta)\left[W_{f_1}(\alpha)-W_{f_2}(\alpha)\ -W_{f_3}(\alpha)+W_{f_1\oplus f_2\oplus f_3}(\alpha)\right] \\ & +\tfrac{1}{4}W_{g_3}(\beta)\left[W_{f_1}(\alpha)-W_{f_2}(\alpha)\ +W_{f_3}(\alpha)-W_{f_1\oplus f_2\oplus f_3}(\alpha)\right] \\ & +\tfrac{1}{4}W_{g_1\oplus g_2\oplus g_3}(\beta)\left[W_{f_1}(\alpha)+W_{f_2}(\alpha)\ -W_{f_3}(\alpha)-W_{f_1\oplus f_2\oplus f_3}(\alpha)\right]. \end{aligned} \tag{7}$$

Since $f_1, f_2,\ f_3$ and $f_1\oplus f_2\oplus f_3$ are t-resilient, we have $W_{f_i}(\alpha)=0$ and $W_{f_1\oplus f_2\oplus f_3}(\alpha)=0$ for any $\alpha\in\mathbb{F}_2^n$ such that $0\le wt(\alpha)\le t$, where $i=1,2,3$. Since $g_1, g_2,\ g_3$ and $g_1\oplus g_2\oplus g_3$ are k-resilient, we have $W_{g_i}(\beta)=0$ and $W_{g_1\oplus g_2\oplus g_3}(\beta)=0$ for any $\beta\in\mathbb{F}_2^m$ such that $0\le wt(\beta)\le k$, where $i=1,2,3$. In addition, we have $wt(\alpha)\le t$ or $wt(\beta)\le k$ if $wt(\alpha,\beta)\le t+k+1$. Further, according to Relation (6), $f(x,y)$ is a $(t+k+1)$-resilient function in $n+m$ variables.

Remark 5 The indirect sum is a particular case of this construction: it corresponds to the case $f_2=f_3$ and $g_2=g_3$.

We modify now the construction of Theorem 2 to ensure a high nonlinearity of the constructed resilient function: to this aim, we assume that the functions f_i are bent (of course, they can then not be balanced and the order t of Theorem 2 is then equal to -1). Before that, we first present a lemma.

Lemma 5 *Let n (>6) be an even positive integer and m be a positive integer. Let $f_1(x), f_2(x)$ and $f_3(x)$ be bent functions in n variables such that $\nu_1=f_1\oplus f_2\oplus f_3$ is a bent function and $\widetilde{\nu_1}=\widetilde{f_1}\oplus\widetilde{f_2}\oplus\widetilde{f_3}$. Let $g_1(y), g_2(y)$ and $g_3(y)$ be functions in m variables. Denote by ν_2 the function $g_1\oplus g_2\oplus g_3$. Let $f(x,y)$ be defined as in Theorem 2 and $\alpha\in\mathbb{F}_2^n, \beta\in\mathbb{F}_2^m$. Then, there are four cases.*

1. *If $W_{f_1}(\alpha)=W_{f_2}(\alpha)=W_{f_3}(\alpha)$, then $W_{\nu_1}(\alpha)=W_{f_1}(\alpha)$. Further,*
$$W_f(\alpha,\beta)=W_{g_1}(\beta)W_{f_1}(\alpha);$$
2. *If $W_{f_1}(\alpha)=W_{f_2}(\alpha)\neq W_{f_3}(\alpha)$, then $W_{\nu_1}(\alpha)=W_{f_3}(\alpha)$. Further,*
$$W_f(\alpha,\beta)=W_{g_1\oplus g_2\oplus g_3}(\beta)W_{f_1}(\alpha);$$
3. *If $W_{f_1}(\alpha)\neq W_{f_2}(\alpha)=W_{f_3}(\alpha)$, then $W_{\nu_1}(\alpha)=W_{f_1}(\alpha)$. Further,*
$$W_f(\alpha,\beta)=W_{g_2}(\beta)W_{f_1}(\alpha);$$

4. If $W_{f_1}(\alpha) = W_{f_3}(\alpha) \neq W_{f_2}(\alpha)$, then $W_{\nu_1}(\alpha) = W_{f_2}(\alpha)$. Further,

$$W_f(\alpha, \beta) = W_{g_3}(\beta) W_{f_1}(\alpha).$$

Proof. Since $\nu_1(x)$ is a bent function in n variables and $\widetilde{\nu_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, then

$$(-1)^{\widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}} = (-1)^{\widetilde{\nu_1}},$$

that is,

$$W_{f_1}(\alpha) W_{f_2}(\alpha) W_{f_3}(\alpha) = 2^n W_{\nu_1}(\alpha). \tag{8}$$

We also know that $W_{f_i}(\alpha) = \pm 2^{n/2}$ for any $\alpha \in \mathbb{F}_2^n$, where $i = 1, 2, 3$. Thus, combining Relations (7) and (8), the conclusion is held.

Theorem 3 *Let n (> 6) be an even positive integer. Let m and k be two integers such that $k < m-1$. Let $f_1(x), f_2(x)$ and $f_3(x)$ be bent functions in n variables. Let $g_1(y), g_2(y)$ and $g_3(y)$ be k-resilient functions in m variables. Denote by ν_1 the function $f_1 \oplus f_2 \oplus f_3$ and by ν_2 the function $g_1 \oplus g_2 \oplus g_3$. If ν_1 is a bent function, ν_2 is a k-resilient function and if $\widetilde{\nu_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, then*

$$\begin{aligned} f(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y) \\ \oplus (f_2 \oplus f_3)(x)(g_2 \oplus g_3)(y) \end{aligned}$$

is a k-resilient function in $n + m$ variables. Further, we have

$$\begin{aligned} N_f \geq 2^{n+m-1} - 2^{n/2-1} \times \max \Bigg\{ & \max_{\beta \in \mathbb{F}_2^m} \{|W_{g_1}(\beta)|\}, \\ \max_{\beta \in \mathbb{F}_2^m} \{|W_{g_2}(\beta)|\}, \max_{\beta \in \mathbb{F}_2^m} \{|W_{g_3}(\beta)|\}, & \max_{\beta \in \mathbb{F}_2^m} \{|W_{\nu_2}(\beta)|\} \Bigg\}; \end{aligned} \tag{9}$$

and the equality holds if and only if $\{f_1, f_1 \oplus 1\} \cap \{f_2, f_2 \oplus 1\} = (\{f_1, f_1 \oplus 1\} \cap \{f_3, f_3 \oplus 1\}) = (\{f_2, f_2 \oplus 1\} \cap \{f_3, f_3 \oplus 1\}) = \emptyset$.

Proof. According to Theorem 2, $f(x, y)$ is a k-resilient function in $n + m$ variables.

Next, we consider the nonlinearity of $f(x, y)$. From Lemma 5, we immediately have

$$\begin{aligned} N_f \geq 2^{n+m-1} - 2^{n/2-1} \times \max \Bigg\{ & \max_{\beta \in \mathbb{F}_2^m} \{|W_{g_1}(\beta)|\}, \\ \max_{\beta \in \mathbb{F}_2^m} \{|W_{g_2}(\beta)|\}, \max_{\beta \in \mathbb{F}_2^m} \{|W_{g_3}(\beta)|\}, & \max_{\beta \in \mathbb{F}_2^m} \{|W_{\nu_2}(\beta)|\} \Bigg\}, \end{aligned}$$

the equality holds if and only if all four cases of Lemma 5 can happen, that is, $\{f_1, f_1 \oplus 1\} \cap \{f_2, f_2 \oplus 1\} = (\{f_1, f_1 \oplus 1\} \cap \{f_3, f_3 \oplus 1\}) = (\{f_2, f_2 \oplus 1\} \cap \{f_3, f_3 \oplus 1) = \emptyset$.

Remark 6 Theorem 3 allows constructing resilient functions offering a compromize between resiliency order (whose ratio with the number of variables is lowered when we move from functions g_i to f) and nonlinearity (which is enhanced thanks to the contribution of the bent functions, resulting in the coefficient $2^{n/2-1}$ in Relation (9)). This is useful cryptographically speaking since low order resilient functions with high nonlinearity are more useful than high order resilient functions (with inevitably low nonlinearity according to the Sarkar-Maitra bound). If the nonlinearity of m-variable resilient functions g_1, g_2, g_3 and $g_1 \oplus g_2 \oplus g_3$ can exceed $2^{m-1} - 2^{\lfloor m/2 \rfloor}$, then the nonlinearity of $f(x, y)$ constructed by Theorem 3 exceeds $2^{n+m-1} - 2^{\lfloor (n+m)/2 \rfloor}$. If m is even, $k > m/2-2$ and g_1, g_2, g_3 and $g_1 \oplus g_2 \oplus g_3$ are m-variable k-resilient functions achieving Sarkar et al's bound, then $N_f = 2^{n+m-1} - 2^{n/2-1+k+1}$; If m is even, $k \leq m/2 - 2$ and g_1, g_2, g_3 and $g_1 \oplus g_2 \oplus g_3$ are m-variable k-resilient functions achieving Sarkar et al's bound (their nonlinearity equal $2^{m-1} - 2^{m/2-1} - 2^{k+1}$), then $N_f = 2^{n+m-1} - 2^{(n+m)/2-1} - 2^{n/2+k+1}$, further, when $n = 6$, we can obtain a $(m+6)$-variable k-resilient function with nonlinearity $2^{6+m-1} - 2^{(6+m)/2-1} - 2^{k+4}$. However, f does not achieve Sarkar et al.'s bound with equality, in general.

Examples of application. In [11, 15] is given an example of functions f_1, f_2, f_3 satisfying a condition which is the same as that needed in Theorem 3. Let $\vartheta(x)$ and $\theta(x)$ be n-variable bent functions. Assume that there exists a vector a such that $D_a\vartheta = D_a\theta$, where $D_a\vartheta(x) = \vartheta(x) \oplus \vartheta(x \oplus a)$ is the so-called derivative of ϑ at a. We can take $f_1(x) = \vartheta(x), f_2(x) = \vartheta(x \oplus a), f_3(x) = \theta(x)$, the hypothesis of Theorem 3 is satisfied: $\nu_1(x) = D_a\vartheta(x) \oplus \theta(x) = D_a\theta(x) \oplus \theta(x) = \theta(x \oplus a)$ is bent and we have $\widetilde{\nu_1}(x) = \widetilde{\theta}(x) \oplus a \cdot x = (\widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3})(x)$.

For example, let $x = (x', x'') \in \mathbb{F}_2^n, x', x'' \in \mathbb{F}_2^{n/2}$. Let ϕ be a permutation on $\mathbb{F}_2^{n/2}$ and ρ_1, ρ_2 be two arbitrary $n/2$-variable Boolean functions. Let us define the M-M bent functions $\vartheta(x) = x' \cdot \phi(x'') \oplus \rho_1(x'')$, $\theta(x) = x' \cdot \phi(x'') \oplus \rho_2(x'')$. Let a' be any nonzero element of $\mathbb{F}_2^{n/2}$ and $a = (a', 0, \ldots, 0) \in \mathbb{F}_2^n$. Thus, we have $D_a\theta = D_a\vartheta$, that is, functions $f_1(x) = \vartheta(x), f_2(x) = \vartheta(x \oplus a), f_3(x) = \theta(x)$ satisfy the condition of Theorem 3.

Remark 7 According to Lemma 5, we know that $W_f(\alpha, \beta) = W_{g_1}(\beta)W_{f_1}(\alpha)$, or $W_{g_2}(\beta)W_{f_1}(\alpha)$, or $W_{g_3}(\beta)W_{f_1}(\alpha)$, or $W_{g_1 \oplus g_2 \oplus g_3}(\beta)W_{f_1}(\alpha)$. Thus, from Theorem 3, an $(n+r)$th-order plateaued function in $n+m$ variables can be obtained if g_1, g_2 , g_3 and $g_1 \oplus g_2 \oplus g_3$ are rth-order plateaued functions.

Another consequence of Lemma 5 is the following secondary construction:

Proposition 2 *Let n (> 6) be an even positive integer. Let m and k be two integers such that $k < m-1$. Let $f_1(x), f_2(x)$ and $f_3(x)$ be bent functions in n variables such that $\nu_1 = f_1 \oplus f_2 \oplus f_3$ is also a bent function and $\widetilde{\nu_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$. Let $p(y)$ and $q(y)$ be two k-resilient functions in m variables. If $W_{f_1}(\mathbf{0}) = W_{f_2}(\mathbf{0}) = W_{f_3}(\mathbf{0})$ or $W_{f_1}(\mathbf{0}) \neq W_{f_2}(\mathbf{0}) = W_{f_3}(\mathbf{0})$, where $\mathbf{0} = (0, 0 \ldots, 0) \in \mathbb{F}_2^n$, then we set $g_1(y) = p(y)$, $g_2(y) = q(y)$ and $g_3(y) = q(y) \oplus y_i$;*
If $W_{f_1}(\mathbf{0}) = W_{f_2}(\mathbf{0}) \neq W_{f_3}(\mathbf{0})$ or $W_{f_1}(\mathbf{0}) = W_{f_3}(\mathbf{0}) \neq W_{f_2}(\mathbf{0})$, then we set $g_1(y) = p(y) \oplus y_i$, $g_2(y) = q(y) \oplus y_i$ and $g_3(y) = q(y)$, where $i \in \{1, 2, \ldots, m\}$. Then, $f(x, y)$, defined as in Theorem 3, is a k-resilient function in $n+m$ variables with nonlinearity:

$$N_f \geq 2^{n+m-1} - 2^{n/2-1} \times \max\left\{\max_{\beta \in \mathbb{F}_2^m}\{|W_p(\beta)|\},\ \max_{\beta \in \mathbb{F}_2^m}\{|W_q(\beta)|\}\right\}, \quad (10)$$

the equality holds if and only if the equality $f_1 = f_2 = f_3$ does not hold.

Proof. Since $p(y)$ (resp. $q(y)$) is a k-resilient m-variable function, the resiliency order of $p(y) \oplus y_i$ (resp. $q(y) \oplus y_i$) is at least $k-1$, that is, $W_{p(y) \oplus y_i}(\beta) = 0$ (resp. $W_{q(y) \oplus y_i}(\beta) = 0$) for any $wt(\beta) \leq k-1$.

From Theorem 3, the function f is at least $(k-1)$-resilient. Now, we prove f is a k-resilient function in $n+m$ variables.

When $W_{f_1}(\mathbf{0}) = W_{f_2}(\mathbf{0}) = W_{f_3}(\mathbf{0})$ or $W_{f_1}(\mathbf{0}) \neq W_{f_2}(\mathbf{0}) = W_{f_3}(\mathbf{0})$, we set $g_1(y) = p(y)$, $g_2(y) = q(y)$ and $g_3(y) = q(y) \oplus y_i$. Thus, g_1 and g_2 are k-resilient functions, g_3 (resp. $g_1 \oplus g_2 \oplus g_3$) is at least $(k-1)$-resilient. Let $(\alpha, \beta) \in \mathbb{F}_2^{n+m}$ and $wt(\alpha, \beta) = k$. There are two different cases to consider.

1. If $wt(\alpha) \geq 1$, then $wt(\beta) \leq k-1$. Moreover, we know that $W_{g_1 \oplus g_2 \oplus g_3}(\beta) = 0$ and $W_{g_3}(\beta) = 0$. Certainly, $W_{g_1}(\beta) = 0$ and $W_{g_2}(\beta) = 0$. From Relation (7), $W_f(\alpha, \beta) = 0$.

2. If $wt(\alpha) = 0$, i.e., $\alpha = \mathbf{0}$, then $wt(\beta) = k$. We know g_1 and g_2 are k-resilient functions, i.e., $W_{g_1}(\beta) = 0$ and $W_{g_2}(\beta) = 0$. According to Lemma 5, we know that $W_f(\alpha, \beta) = W_{g_1}(\beta) W_{f_1}(\alpha)$ (resp. $W_f(\alpha, \beta) = W_{g_2}(\beta) W_{f_1}(\alpha)$) if $W_{f_1}(\alpha) = W_{f_2}(\alpha) = W_{f_3}(\alpha)$ (resp. $W_{f_1}(\alpha) \neq W_{f_2}(\alpha) = W_{f_3}(\alpha)$). Thus, we have that $W_f(\alpha, \beta) = 0$.

When $W_{f_1}(\mathbf{0}) = W_{f_2}(\mathbf{0}) \neq W_{f_3}(\mathbf{0})$ or $W_{f_1}(\mathbf{0}) = W_{f_3}(\mathbf{0}) \neq W_{f_2}(\mathbf{0})$, we set $g_1(y) = p(y) \oplus y_i$, $g_2(y) = q(y) \oplus y_i$ and $g_3(y) = q(y)$. We can prove $W_f(\alpha, \beta) = 0$ for $wt(\alpha, \beta) = k$ by using the same method as above.

Relation (10) is then straightforward. From Lemma 5, the equality of Relation (10) holds if and only if the equality $f_1 = f_2 = f_3$ does not hold.

Remark 8 If $N_p = N_q$, then $N_f = 2^{n+m-1} - 2^{n/2-1} \times \max\limits_{\beta \in \mathbb{F}_2^m} \{|W_p(\beta)|\}$. If we choose $p(y), q(y)$ from PW functions (Patterson and Wiedemann in [35] proposed 15-variable Boolean functions with nonlinearity $2^{14} - 2^7 + 2^4 + 2^2$, which are called PW functions), then an $(n+15)$-variable function with nonlinearity $2^{n+15-1} - 2^{n/2+7-1} + 2^{n/2+4-1} + 2^{n/2+2-1}$ can be obtained by Proposition 2. The nonlinearity of functions constructed by this way is the best known. In addition, if we apply direct sum (resp. indirect sum) using as initial functions $p(y)$ and $f_i(x)$ (resp. $p(y), q(y)$, $f_i(x)$ and $f_j(x)$), where $i, j = 1, 2, 3, i \neq j$, then the nonlinearity of functions constructed this way equals $2^{n+m-1} - 2^{n/2-1} \times \max\limits_{\beta \in \mathbb{F}_2^m} \{|W_p(\beta)|\}$ as well. If we do not consider the resilience of the constructed function $f(x, y)$, then we can set $g_1(y) = p(y), g_2(y) = q(y)$ and $g_3(y) = q(y) \oplus l(y)$, where $l(y) \in A_m$.

In [21], Fu et al. proposed a method for constructing k-resilient functions in odd numbers of variables. For odd $n \geq 35, k = 1$ (resp. $n \geq 39, k = 2$), a large class of k-resilient n-variable functions, whose nonlinearity is the best known, can be constructed by the method. From their construction [21, Construction], we found that the direct sum functions were chosen initial functions. Here, if we substitute the functions constructed by Proposition 2 for the direct sum functions, then many resilient functions on odd number of variables whose nonlinearities equal those of the functions presented by Fu et al. in [21] can be obtained.

Example 1 *Several constructions of 8-variable 1-resilient functions with nonlinearity* 116 *were presented in [17, 27, 28, 29]. By using two different* 1*-resilient* 8*-variable functions and three* 6*-variable bent functions* f_1, f_2, f_3 *(which satisfy* $f_1 \oplus f_2 \oplus f_3$ *being also bent and* $\widetilde{f_1 \oplus f_2 \oplus f_3} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$*), with Proposition 2, we can obtain* 14*-variable 1-resilient functions with nonlinearity* $2^{13} - 2^6 - 2^5 = 8096$. *The functions* $(14, 1, -, 8096)$ *earlier known could only be obtained by direct sum and indirect sum.*

Clearly, the functions constructed by Proposition 2 are different from those constructed by direct sum. In Table 1, we describe the difference between the functions constructed by Proposition 2 and the functions constructed by indirect sum.

5 Conclusion

Bent functions and resilient functions with high nonlinearity are actively studied for their numerous applications in cryptography, coding theory, and

Table 1: Forms of Functions Constructed by Indirect Sum and Proposition 2

Initial Functions	Indirect sum	Proposition 2
$f_1 \neq f_2, f_2 \neq f_3$, $f_1 \neq f_3$, $g_1 \neq g_2$, $g_3 = g_2 \oplus y_i$	$f_1(x) \oplus g_1(y) \oplus$ $(f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$	$f_1(x) \oplus g_1(y) \oplus$ $(f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$ $\oplus y_i(f_2 \oplus f_3)(x)$
$f_1 \neq f_2, f_2 \neq f_3$, $f_1 = f_3$,$g_1 \neq g_2$, $g_3 = g_2 \oplus y_i$	$f_1(x) \oplus g_1(y) \oplus$ $(f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$	$f_1(x) \oplus g_1(y) \oplus$ $(f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$ $\oplus y_i(f_1 \oplus f_2)(x)$

other fields.

In this paper, we focused on the constructions of both bent functions and highly nonlinear Boolean functions. We first presented a novel secondary construction of bent functions. By using this method, we could deduce several concrete constructions of bent functions from known bent functions. In addition, we presented a generalization of the indirect sum construction for constructing resilient functions with high nonlinearity.

6 Acknowledgment

This work was supported in part by National Science Foundation of China (60833008, 61173152), and in part Science and Technology on Communication Security Laboratory (9140C110201110C1102).

References

[1] P. Camion, C. Carlet, P. Charpin and N. Sendrier, " On correlation-immune functions," in *Advances in Cryptology-CRYPTO'91 (Lecture Notes in Computer Sceince)*, J. Feigenbaum, Ed. Berlin, Germany: Springer-Verlag, 1991, vol. 576, pp. 86–100.

[2] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," in *Advances in EUROCRYPT2000 (Lecture Notes in Computer Sceince)*, B. Preneel, Ed. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 573–588.

[3] C. Carlet, “Two new classes of bent functions,” in *Advances in EUROCRYPT’93 (Lecture Notes in Computer Sceince)*, T. Helleseth, Ed. Berlin, Germany: Springer-Verlag, 1994, vol. 765, pp. 77–101.

[4] C. Carlet, “ Generalized partial spreads,” *IEEE Trans. Inf. Theory*, vol. 41, no. 5 pp. 1482–1487, Sep. 1995.

[5] C. Carlet, “A construction of bent functions,” in *Proc. third international conference on Finite fields and applications*, S. Cohen and H. Niederreiter, Eds. Cambridge University Press, pp. 47–58, 1996.

[6] C. Carlet, “On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions,” in *Proc. of SETA’01 (Sequences and their Applications 2001), Discrete Mathematics and Theoretical Computer Science*, Berlin, Germany: Springer-Verlag, 2001, pp. 131–144.

[7] C. Carlet, “A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland constructions,” in *Advances in Cryptology-CRYPTO2002 (Lecture Notes in Computer Sceince)*, Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 549–564.

[8] C. Carlet, “On the confusion and diffusion properties of Maiorana-McFarland’s and extended Maiorana- McFarland’s functions,” *J. Complexity*, vol. 20, no. 2-3 pp. 182–204, 2004.

[9] C. Carlet, “On the secondary constructions of resilient and bent functions,” in *Proc. the Workshop on Coding, Cryptography and Combinatorics 2003*, K. Feng, H. Niederreiter and C. Xing, Eds. published by Birkhäuser Verlag, 2004, pp. 3–28.

[10] C. Carlet, “Concatenating indicators of ats for designing cryptographic functions,” *Des. Codes Cryptogr.*, vol. 36, no. 2, pp. 189–202, 2005.

[11] C. Carlet, “On bent and highly nonlinear balanced/resilient functions and their algebraic immunities,” in *Proc. AAECC 2006 (Lecture Notes in Computer Science)*, M. Fossorier et al. Eds. Berlin, Germany: Springer-Verlag, 2006, vol. 3857, pp. 1–28.

[12] C. Carlet, “Boolean Functions for Cryptography and Error Correcting Codes,” in *Monography “Boolean Models and Methods in Mathematics, Computer Science, and Engineering*”, Y. Crama and P. Hammer, Eds. Cambridge University Press, 2010, pp. 257–397.

[13] C. Carlet, H. Dobbertin and G. Leander, "Normal extensions of bent functions," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2880–2885, Nov. 2004.

[14] C. Carlet and P. Sarkar, "Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions," *Finite fields and Applications*, vol. 8, pp. 120–130, Aug. 2002.

[15] C. Carlet and J. L. Yucas, "Piecewise Constructions of Bent and Almost Optimal Boolean Functions," *Des. Codes Cryptogr.*, vol. 37, no. 3, pp. 449–464, 2005.

[16] C. Carlet, F. Zhang and Y. Hu, "Secondary constructions of bent functions and their enforcement," *Advances in Mathematics of Communications*, vol. 6, no. 3, pp. 305–314, 2012.

[17] J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan, "Evolving Boolean Functions Satisfying Multiple Criteria," in *Proc. INDOCRYPT 2002 (Lecture Notes in Computer Science)*, A. Menezes, P. Sarkar, Eds. Berlin, Germany: Springer-Verlag, 2002, vol. 2551, pp. 246–259.

[18] J. Dillon, "Elementary Hadamard difference sets", Ph.D. dissertation, Univ. Maryland, College Park, 1974.

[19] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Proc. FSE 1995 (Lecture Notes in Computer Science)*, H. Gilbert, H. Handschuh, Eds. Berlin, Germany: Springer-Verlag, 2006, vol. 1008, pp. 61–74.

[20] H. Dobbertin and G. Leander, "Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions," *Des. Codes Cryptogr.*, vol. 49, no. 1-3, pp. 3–22, 2008.

[21] S. Fu, C. Li, k. Matsuura and L. Qu, "Consturciton of odd-varibale resilient Boolean functions with optimal degree," *IEICE Transactions on Fundamentals*, vol. E94-A: pp. 265–267, 2011.

[22] S. Fu, K. Matsuura, C. Li, L. Qu," Results on High Nonlinearity Resilient S-Boxes with Given Degree," *Des. Codes Cryptogr.*, vol. 64, no. 3, pp. 241–253, 2012.

[23] P. Guillot, "Completed GPS Covers All Bent Functions," *J. Combin. Theory Ser. A*, vol. 93, pp. 242–260, 2001.

[24] G. Leander and G. McGuire, "Construction of bent functions from near-bent functions," *J. Combin. Theory Ser. A*, vol. 116, pp. 960–970, 2009.

[25] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 865–868, Nov. 1982.

[26] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing company, Amsterdam, 1977.

[27] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1825–1834, July 2002.

[28] S. Maity and T. Johansson, "Construction of Cryptographically Important Boolean Functions," in *Proc. INDOCRYPT 2002 (Lecture Notes in Computer Science)*, A. Menezes, P. Sarkar, Eds. Berlin, Germany: Springer-Verlag, 2002, vol. 2551, pp. 234–245.

[29] S. Maity and S. Maitra, "Minimum Distance between bent and 1-resilient Boolean functions," in *Proc. FSE 2004 (Lecture Notes in Computer Science)*, B. K. Roy, W. Meier, Eds. Berlin, Germany: Springer-Verlag, 2004, vol. 3017, pp. 143–160.

[30] R. I. McFarland, " A family of difference sets in non-cyclic groups," *J. Comb. Theory, Ser.A.*, vol. 15, pp. 1–10, 1973.

[31] Q. Meng, L. Chen and F. Fu, "On homogeneous rotation symmetric bent functions," *Discrete Appl. Math.*, vol. 158, pp. 1111–1117, 2010.

[32] J. S. No, G. M. Gil and D. J. Shin, "Generalized Construction of Binary Bent Sequences With Optimal Correlation Property," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 858–864, June 1982.

[33] J. D. Olsen, R. A. Scholtz and L. R. Welch, "Bent-function sequence," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 1769–1780, July 2003.

[34] E. Pasalic, " Maiorana-McFarland class: degree optimization and algebraic properties," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4581–4594, Oct. 2006.

[35] N. J. Patterson and D. H. Wiedemann, "The covering radius of the (215, 16) Reed-Muller code is at least 16276," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp.354–356, Mar. 1983.

[36] O. S. Rothaus, "On "bent" functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.

[37] P. Sarkar and S. Maitra, "Nonlinearity Bounds and Constructions of Resilient Boolean Functions," in *Advances in Cryptology-CRYPTO 2000 (Lecture Notes in Computer Science)*, M. Bellare, Ed. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 515–532.

[38] J. Seberry, X-.M. Zhang and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," in *Advances in Cryptology-CRYPTO'93 (Lecture Notes in Computer Science)*, D. R. Stinson, Ed. Berlin, Germany: Springer-Verlag, 1994, vol. 773, pp. 49–60.

[39] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. 30, no. 5 pp. 776–780, May 1984.

[40] Y. V. Tarannikov, "On resilient Boolean functions with maximum possible nonlinearity," in *Proc. of INDOCRYPT 2000 (Lecture Notes in Computer Science)*, B. K. Roy, E. Okamoto, Eds. Berlin, Germany: Springer-Verlag, 2000, vol. 1977, pp. 19–30.

[41] J. Wolfmann, "Bent functions and coding theory," in *Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth and D. Jungnickel, Eds. Amsterdam: Kluwer, pp. 393–417, 1999.

[42] G. Xiao and J. L. Massey, " A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 569–571, Mar. 1988.

[43] X. Y. Zeng and L. Hu, "Constructing Boolean Functions by Modifying Maiorana-McFarland's super-class Functions," *IEICE TRANS.FUNDAMENTALS*, vol. E88-A, pp. 59–66, 2005.

[44] F. Zhang, Y. Hu, M. Xie and Y. Wei, "Constructions of 1-Resilient Boolean Functions on Odd Number of Variables with a High Nonlinearity," *Security and Communication Networks*, vol. 5, no. 6, pp. 614–624, 2012.

[45] F. Zhang, Y. Hu, Y. Jia and M. Xie, "New Constructions of Balanced Boolean Functions with High Nonlinearity and Optimal Algebraic De-

gree," *International Journal of Computer Mathematics*, vol. 89, no. 10, pp. 1319–1331, 2012.

[46] W. G. Zhang and G. Z. Xiao, "Constructions of Almost Optimal Resilient Boolean Functions on Large Even Number of Variables," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5822–5831, Dec. 2009.

[47] Y. Zheng and X.-M. Zhang, "Relationships between bent functions and complementary plateaued functions," in *Proc. 2nd Int. Conf. Information Security and Cryptology (ICISC'99) (Lecture Notes in Computer Science)*, J. Song Ed. Berlin, Heidelberg, New York: Springer-Verlag, 1999 vol. 1787, pp. 60–75.

[48] Y. Zheng and X.-M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions," *Proc. of Selected Areas in Cryptolgraphy 2000 (Lecture Notes in Computer Science)*, D.R. Stinson and S. Tavares, Eds. Berlin, Germany: Springer-Verlag, 2001, vol. 2012, pp. 262–274.